Author Index for Refereed Articles in Vol. 9

Abrams, M. D., 699

Badenhorst, K. P., 339
Bell, G. G., 621
Bosselaers, A., 257
Bürk, H., 715
Burns, J., 67

Carroll, J. M., 613
Cole, R., 319

Domingo-Ferrer, J., 145

Eloff, J. H. P., 339

Govaerts, R., 257

Haga, W. J., 723
Harn, L., 539
Herschberg, I. S., 161
Higginson, G. O., 621
Hoge, J. C., 153
Huguet-Rotger, L., 145

Jones, S. K., 411

Laferriere, C., 235, 621
Lin, H.-Y., 539
Lloyd, I., 419

McKosky, R. A., 431
Mercer, L. C. J., 59, 331
Micucci, V. A., 153
Mitchell, C. J., 67
Muftic, S., 245

Olson, I. M., 699

Paans, R., 161
Parker, T. A., 519
Patel, A., 631
Pfitzmann, A., 715
Preneel, B., 257

Ramaswamy, R., 77

Sanders, P. W., 631
Shepherd, S. J., 631
Shiva, S. G., 431
Smulders, P., 53

Vandewalle, J., 257

White, Jr., C. E., 411
Wiseman, S., 529

Zviran, M., 153, 723

Computers & Security, 9 (1990) 753-756

Subject Index for Refereed Articles in Vol. 9

A posteriori security system
  a file integrity checking system to detect and recover from program modification attacks in multi-user computer systems, 431
Access control
  application access control standards for distributed systems, 519
Access control policy
  computer access control policy choices, 699
Agents
  a comprehensive security system — the concepts, agents and protocols, 631
Applications data
  fraud detection via regression analysis, 331
Assurance
  software evaluation in high integrity systems, 419
Auditing a change
  auditing the change management process, 161
Authentication
  application access control standards for distributed systems, 519
  cognitive passwords: the key to easy access control, 723
  a security scheme for resource sharing over a network, 67
Authentication protocols
  secure network bootstrapping: an algorithm for authentic key exchange and digital signatures, 145
Authority
  computer access control policy choices, 699

Beacons
  transaction protection by "antennas", 245
Binary-derivative testing
  "do-it-yourself" cryptography, 613
Block ciphers
  "do-it-yourself" cryptography, 613

Cashless payment
  value exchange systems enabling security and unobservability, 715
Change management
  auditing the change management process, 161
Cognitive passwords
  cognitive passwords: the key to easy access control, 723
Computer fraud
  fraud detection via regression analysis, 331
  tailor-made auditing of information systems for the detection of fraud, 59
Computer networks
  a comprehensive security system — the concepts, agents and protocols, 631
  secure network bootstrapping: an algorithm for authentic key exchange and digital signatures, 145
  a security scheme for resource sharing over a network, 67
Computer security
  computer security methodology: risk analysis and project definition, 339
Computer viruses
  a file integrity checking system to detect and recover from program modification attacks in multi-user computer systems, 431
  the IPM model of computer virus management, 411
Covert chanels
  control of confidentiality in databases, 529
Cryptographic checksum
  cryptanalysis of a fast cryptographic checksum algorithm, 257
Cryptographic scheme
  a cryptographic key generation scheme for multilevel data security, 539
Cryptography
  crytanalysis of a fast cryptographic checksum algorithm, 257

Subject Index

secure network boostrapping: an algorithm for authentic key exchange and digital signatures, 145
a security scheme for resource sharing over a network, 67

Database security
control of confidentiality in databases, 529
Decision support system (DSS)
SPAN — a DSS for security plan analysis, 153
Detective control
fraud detection via regression analysis, 331
Digital payment system
value exchange systems enabling security and unobservability, 715
Digital pseudonyms
value exchange systems enabling security and unobservability, 715
Digital signatures
secure network bootstrapping: an algorithm for authentic key exchange and digital signatures, 145
Distributed systems
application access control standards for distributed systems, 519
a model for security in distributed systems, 319

Eavesdropping risks
the threat of information theft by reception of electromagnetic radiation from RS-232 cables, 53
ECMA
a model for security in distributed systems, 319
EDP-audit
auditing the change management process, 161
fraud detection via regression analysis, 331
tailor-made auditing of information systems for the detection of fraud, 59
Electromagnetic radiation
the threat of information theft by reception of electromagnetic radiation from RS-232 cables, 53

File integrity
a file integrity checking system to detect and recover from program modification attacks in multi-user computer systems, 431

Fraud detection
fraud detection via regression analysis, 331
tailor-made auditing of information systems for the detection of fraud, 59

Generalized framework for access control
computer access control policy choices, 699

Hierarchy of control
computer access control policy choices, 699
High integrity
software evaluation in high integrity systems, 419

Identification by third parties
value exchange systems enabling security and unobservability, 715
Inference
control of confidentiality in databases, 529
Information protection
cryptanalysis of a fast cryptographic checksum algorithm, 257
Integrity
cryptanalysis of a fast cryptographic checksum algorithm, 257
the IPM model of computer virus management, 411
Internal control
auditing the change management process, 161
Interworking
application access control standards for distributed systems, 519
IS security
SPAN — a DSS for security plan analysis, 153

Key distribution
a cryptographic key generation scheme for multilevel data security, 539
Key distribution centre
a key management algorithm for secure communication in open systems inerconnection architecture, 77
Key exchange
secure network bootstrapping: an algorithm for authentic key exchange and digital signatures, 145

Key management
a key management algorithm for secure communication in open systems inerconnection architecture, 77

Message authentication code
cryptanalysis of a fast cryptographic checksum algorithm, 257
Methodology
computer security methodology: risk analysis and project definition, 339
Multi-level secure text DBMS
security architectures for textual databases, 621
Multilevel data security
a cryptographic key generation scheme for multilevel data security, 539
Mutually suspicious users
transaction protection by "antennas", 245

Network security
secure network bootstrapping: an algorithm for authentic key exchange and digitial signatures, 145

Open systems interconnection (OSI) architecture
a key management algorithm for secure communication in open systems inerconnection architecture, 77

Partially ordered hierarchy
a cryptographic key generation scheme for multilevel data security, 539
Passwords
cognitive passwords: the key to easy access control, 723
Policy
a comprehensive security system — the concepts, agents and protocols, 631
Polyinstantiation
control of confidentiality in databases, 529
Prevention
the IPM model of computer virus management, 411
Preventive control
tailor-made auditing of information systems for the detection of fraud, 59

Protocol data units
a key management algorithm for secure communication in open systems inerconnection architecture, 77
Protocols
a comprehensive security system — the concepts, agents and protocols, 631
a security scheme for resource sharing over a network, 67

Random-number generation
"do-it-yourself" cryptography, 613
Regression analysis
fraud detection via regression analysis, 331
Restore procedures
auditing the change management process, 161
Risk analysis
computer security methodology: risk analysis and project definition, 339
Risk assessment
SPAN — a DSS for security plan analysis, 153
RS-232 cable
the threat of information theft by reception of electromagnetic radiation from RS-232 cables, 53
RSA scheme
a cryptographic key generation scheme for multilevel data security, 539

Secure communication
a key management algorithm for secure communication in open systems inerconnection architecture, 77
Secure DBMS
a discussion of implementation strategies for secure database management systems, 235
Security
application access control standards for distributed systems, 519
auditing the change management process, 161
a comprehensive security system — the concepts, agents and protocols, 631
a discussion of implementation strategies for secure database management systems, 235
the IPM model of computer virus management, 411

Subject Index

a security scheme for resource sharing over a network, 67

Security architecture

a discussion of implementation strategies for secure database management systems, 235

a model for security in distributed systems, 319

security architecture for textual databases, 621

Security information

a model for security in distributed systems, 319

Security management

a comprehensive security system — the concepts, agents and protocols, 631

Security models

a model for security in distributed systems, 319

software evaluation in high integrity systems, 419

Security planning

SPAN — a DSS for security plan analysis, 153

Security policy

software evaluation in high integrity systems, 419

Security protocols

transaction protection by "antennas", 245

Security services

transaction protection by "antennas", 245

Software security

software evaluation in high integrity systems, 419

Standards

application access control standards for distributed systems, 519

a model for security in distribution systems, 319

Stream ciphers

"do-it-yourself" cryptography, 613

Symmetric ciphers

"do-it-yourself" cryptography, 613

System security

software evaluation in high integrity systems, 419

Systems management

the IPM model of computer virus management, 411

Text DBMS

security architecture for textual databases, 621

Transport protocol

a key management algorithm for secure communication in open systems inerconnection architecture, 77

Trust

a model for security in distributed systems, 319

Trustee

value exchange systems enabling security and unobservability, 715

Unobservable value exchange

value exchange systems enabling security and unobservability, 715

User identification

cognitive passwords: the key to easy access control, 723

User-modified algorithms

"do-it-yourself" cryptography, 613